HIPAA Privacy Regulations

The Basics

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Topics

- Background
- Applicability
- Compliance
- Use and Disclosure
- Standards with Organizational Impacts
- Individual Rights
- Standards with Administrative Impacts

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Background

A Brief History

- November 3, 1999 - proposed privacy regulations
- December 28, 2000 - published in *Federal Register*
- January 23, 2001 - effective date delayed
- February 13, 2001 - Congressional review begins
- March 2, 2001 - New 30 day comment period opens
- April 14, 2001 - rule becomes effective
- April 14, 2003 - compliance date (extra year for small health plans)
- July, 2001 - HHS offers clarifications
- Remainder 2001 - rule modifications?

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Background

Some Context

Privacy protections exist through a patchwork of

- Federal, state and local law
- Contractual obligations
- Industry custom and practice

Security vs. Privacy

- Security rules deal with how data is stored and accessed
- Privacy rules deal with how and to whom data is disclosed

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Applicability

Who is Subject to this rule?

Covered Entities (direct)

- Health plans
- Health care clearinghouses
- Health care providers who electronically transmit any health information in a HIPAA-covered “transaction”

Business Associates (contractual)

- Performs a function for or on behalf of a covered entity

and

- Receives Protected Health Information from a covered entity

Applicability

Special Covered Entities

Hybrid Entities

- Single legal entity that is a covered entity
- Covered functions are not its primary functions
- Firewall — disclosure to other components must meet requirements

Multi-Function Entities

- Single legal entity with a combination of provider, plan or clearinghouse operations
- A health care component may not share protected information with other components

  - Provider component cannot share patient information with health plan component if patient not in the plan

Applicability

Special Covered Entities

Affiliated Covered Entities

- Legally separate covered entities with common ownership and control
- May designate themselves as a single covered entity
- Component rules apply

Organized Health Care Arrangement

- Separate covered entities
- Establish clinically and operationally integrated systems
- Permitted to share information for treatment, management and operations
- May use common notice and consent

Applicability

Preemption of Contrary State Law

Contrary Means:

- A covered entity would find it impossible to comply with both the State and federal requirements;

  or

- The provision of State law stands as an obstacle to the accomplishment and execution of the full purpose and objectives of:
  - HIPAA privacy provisions (PL 104-191 - Sec. 264)
  - Administrative Simplification provisions of the Social Security Act (Title XI - Part C)

Applicability

Preemption of State Law

Contrary State laws are preempted by HIPAA unless:

HHS Secretary determines State law is necessary
(A)

- to prevent fraud and abuse*
- to regulate insurance and health plans*
- for reporting of state health care delivery and costs*
- for public health, safety or welfare & determines that privacy intrusion is warranted

or

(B)

- has as its principal purpose the regulation of controlled substances*

Applicability

Preemption of State Law

Contrary State laws are preempted unless:

- State law privacy provisions are more stringent*
- State provisions provide for reporting of disease, injury, child abuse, birth, death, public health surveillance, public health investigations or interventions*
- State law requires health plans to report or provide access to information for management and financial audits, program monitoring or the licensure or certification of facilities or individuals*

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Compliance

Enforcement

Office of Civil Rights (DHHS)

Receive and investigate complaints
Conduct compliance reviews

Covered entities must

Provide records and compliance report
Cooperate with investigations and reviews

Enforcement regulations

coming later this year?

Compliance

Statutory Penalties

Civil penalties

- $100 per violation
- Annual cap: Total penalties not to exceed $25,000 per year for all violations of a single requirement or prohibition

Criminal penalties

- Wrongful disclosure — up to $5,000 and/or 1 year jail time
- False pretenses — up to $100,000 and/or 5 yrs imprisonment
- For profit/with malice — up to $250,000 and/or 10 yrs in jail

Compliance

Penalties Required by Rule

Internal Sanctions

- Covered entities must develop and apply sanctions for failure to abide by company policies and/or the HIPAA regulations
- Workforce sanctions may range from “warning to termination” at covered entities discretion
- Covered entity sanctions apply to business associates via contract
  - no monitoring necessary, action taken only when known
  - expected to investigate complaints
  - take reasonable steps to cure breach or terminate contract
  - notify Secretary if termination not feasible

Compliance

Responsibilities of Covered Entities

No enforcement rule yet, but current final rules require covered entities to:

- Keep record and submit compliance reports as determined by the Secretary
- Cooperate with the Secretary
- Permit access to records by Secretary
- Certify what efforts have been made to obtain required information from others

Compliance

Complaints to the Secretary

Complaints:

- Filed, in writing, within 180 days of when violation known

Investigations:

- Secretary may investigate complaints

Compliance Reviews:

- Secretary may conduct reviews to determine whether covered entities are complying with requirements

Secretarial Actions:

- non-compliance - will attempt to resolve
  - first informally
  - still unresolved - issue findings documenting non-compliance
- no violation - will notify that no further action necessary

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Use and Disclosure

Covered Information

Individually Identifiable Health Information (IIHI)

- Any health information relating to
  - Past, present or future physical or mental health or condition
  - Provision of health care or
  - Past, present or future payment for health care
- Created/received by provider, plan, employer or clearinghouse
- Individually identifiable or there is a reasonable basis to believe the information can be used to identify the individual

Applicability

Covered Information

Protected Health Information (PHI)

- IIHI that is:

  Transmitted by electronic media;
  Maintained in any electronic medium; or
  Transmitted or maintained in any other form or medium

- Any other form or medium means:

  Written
  Verbal
  Evolving forms of data capture and transmission not comprehended by the definition of “electronic”

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Use and Disclosure

General Rules

A covered entity may not use or disclose protected health information, except as permitted or required.

Permitted:

- To the individual who is the subject of the information
- Basically anything an individual "permits"
  - "Consent"
  - Other agreement
  - "Authorization"

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Use and Disclosure

Individual Permissions

Permission Type	Applies to	Requirements
Consent	For treatment, payment and health care operations	- Obtained by direct treatment provider - May condition care upon receiving
Opportunity to Agree/Object	- Facility directories available for inquiry - Notification of others	- Verbal agreement OK - Then document
Authorization	- Everything Else	- Written - Specific Content - Treatment may Not be conditioned on receipt - Revocable

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Use and Disclosure

Exceptions

Permitted exceptions not needing an individual's "permission":

- Required by law
- Public health
- Reports to government authorities of abuse, neglect or domestic violence
- Law enforcement
- Judicial and administrative proceedings
- Health oversight activities
- Avert imminent threat to health or safety of a person or public
- Specialized government functions
- worker's compensation
- Organ donation or transplantation
- Coroners and medical examiners

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Use and Disclosure

Required

- To individual upon the individual's request
  notable exceptions:
  - ongoing civil, criminal, administrative proceedings
  - inmate's request
  - psychotherapy notes
  - as required by law
- To individual's request for an accounting of disclosures
  notable exceptions:
  - treatment, payment, operations
  - persons involved in care
  - correctional institutions or law enforcement
- To HHS in connection with its enforcement and compliance reviews

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

Consent

- Required for providers, optional for health plans
- Individual's "consent," prior to use or disclosure, for treatment, payment or health care operations
- May condition treatment/enrollment on consent
- Exceptions:
  - Emergency treatment situations
  - Care required by law but unable to obtain consent (after attempt)
  - Providers with "indirect relationship" to patient
  - Inmates of correctional facilities
  - Substantial communication barriers with inferred consent

Organizational Impacts

Consent: Specifications

- Content
  - Use and disclose for treatment, payment and operations
  - Refer to notice of privacy practices
  - Rights to request limitations or revoke consent
  - Signed and dated by individual
- Can be brief and written in general terms
- Must document failure to obtain consent and reasons
- Defective consent = no consent
- Joint consents for organized health care arrangement

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

Authorization

- If not otherwise permitted, must obtain individual's "authorization" for use or disclosure
- A customized document giving permission to use specified PHI for specified purposes
  - May NOT condition treatment on authorization (except clinical trials)
  - covers only the uses and disclosures stipulated
  - Individual may revoke at any time
  - Applies to all covered entities, not just providers
- *Must* be obtained for any use or disclosure of psychotherapy notes with few exceptions

Organizational Impacts

Authorization: Specifications

- Required elements:
  - Specific description of information
  - Persons authorized to disclose
  - Persons to whom disclosure may be made
  - Right to revoke
  - Information subject to redisclosure
  - Signature and date
  - Expiration date
- Given for specific period of time
- Plain language
- Defective authorization is not valid

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

Minimum Necessary

- Amount of information (PHI) disclosed is restricted to the minimum amount necessary to accomplish intended purpose
- Must make “reasonable efforts” to limit:
  - Identify persons or classes of persons in workforce needing access
  - Identify the category(s) of PHI to which access is needed
  - limit access to those identified
- Policies and procedures for recurring and routine disclosures
- Must have process to review non-routine requests on a case-by-case basis
- Must also abide by any agreed upon restrictions requested by the individual

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

Minimum Necessary

- Exceptions:
  - Disclosure among providers for treatment
  - Release authorized by or for individual's own review
  - Disclosure to HHS
  - Compliance with HIPAA requirements
  - Required by law
- Impact considerations:
  - Non-treatment uses; "reasonableness" Phone, fax, e-mail disclosures
  - Applications: reports, user screens and e-forms, integrated databases
  - Justifying release of entire medical record - explicitly stated in policy
  - Case by case review of non-standard requests
  - Applications for federal or state benefits
    Authorizations permitting disclosures to agencies for eligibility determinations

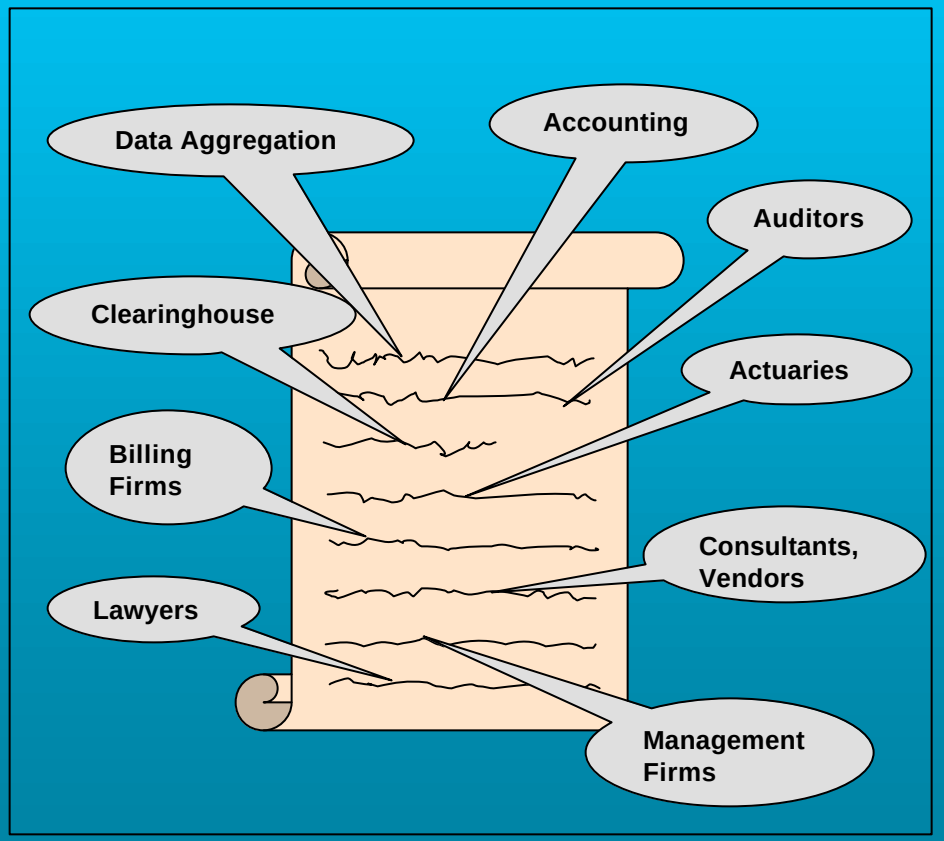
HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

Business Associates

A person who, on behalf of a covered entity - -

- Performs or assists with a function or activity involving:
  - Individually identifiable information, or
  - Otherwise covered by HIPAA
- Performs certain identified services



HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

Business Associates

- A covered entity may allow a business associates to create or obtain PHI if it obtains satisfactory assurance that business associates will appropriately safeguard the information
  - "Assurance" received through contracts between business associates and covered entity
  - Covered entity need not monitor or oversee means by which business associates carry out contract
- If covered entity knows of a pattern of activity constituting a breach by the business associate, then
  - Must take reasonable steps to cure
  - If unsuccessful, must terminate contract
  - If not feasible to terminate, must report to DHHS
  - Otherwise, considered violation by covered entity

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

Business Associate Contracts

- Comply with permitted uses or disclosures requirements
- No further use or disclosure other than what is contracted or required by law
- Implement appropriate privacy and security safeguards
- Ensure its subcontractors comply with same contractual conditions and restrictions
- Report unauthorized disclosures to covered entity - including subcontractors
- Make protected health information available in accordance with individual rights of access
- Make its records available to HHS for determination of covered entity's compliance
- Return or destroy all protected health information upon termination of arrangement, if feasible

Organizational Impacts

Business Associates

If covered entity and BA are both governmental entities:

- Covered entity may use a MOU containing HIPAA compliant terms
- Covered entity is compliant if other law accomplishes HIPAA contract objectives:
  - Includes regulations adopted by the covered entity or its BA
- If the BA relationship is required by law, the covered entity may disclose without meeting HIPAA contract requirements providing
  - attempts to obtain satisfactory assurances in MOU
  - documents failed attempts and reasons assurances cannot be obtained
  - may omit termination authorization if inconsistent with legal obligations of either entity

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Organizational Impacts

De-identified PHI

Use and disclosure restrictions do not apply to de-identified information

- Does not identify an individual (and no key to re-identify may be disclosed)

Covered entity may determine not individually identifiable only by:

(1) a person knowledgeable in statistical and scientific principles determines that there is no reason to believe recipient could identify individual alone or in combination with other information

Or

(2) The safe harbor approach: Removal of all specific identifiers (18), such as:

Names of person, relatives, employers
Address, phone number, fax, email
Social security, plan, account, record numbers

Individual Rights

Right to Notice of Privacy Practices

- Be written in plain language with example(s) of permitted use and disclosure
- Describe purposes not needing consent or authorization
- Describe more stringent use and disclosure law
- Include a statements regarding:
  - individual rights to access, inspection, accounting
  - covered entities duties
  - complaints and contacts
  - effective date
- An inmate does not have a right to notice under HIPAA

Individual Rights

Provision of Notice

Health Plan

At time of enrollment

Within 60 days of a revision

Not less than every three years

Provider

No later than date of first service delivery

Have available for pick-up

Post in a clear and prominent location

When revised, make available on revision effective date

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Individual Rights

Right to Access and Amend

Right to access own PHI

- Inspect and copy for as long as PHI is maintained
- Provide access in form or format requested
- Summary of information if individual agrees in advance
- Some exclusions
- Other -- denying access

Right to amend own PHI

- Accepting amendment
  - Inform individual & amend
  - Distribute to prior recipients
- Denying amendment
  - Not created by covered entity
  - Covered entity believes PHI is accurate and complete
  - Denial letter, statement of disagreement, rebuttal

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Individual Rights

Right to Receive an Accounting of Disclosures

- Covered entity accounts for disclosures in the six years prior to request
  - Date and purpose of disclosure
  - Recipient name and address
  - Description of information disclosed
  - Statement of the purpose of the disclosure
  - Provide accounting within 60 days of request
  - Document above + titles or offices processing requests
- Exceptions:
  - Treatment, payment and health care operations
  - To the individual or those involved in care
  - Facility directories
  - Correctional institutions,
  - Health oversight or law enforcement agencies if impedes activities

    Temporary suspension - no longer than 30 days

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Individual Rights

Other Rights

Right to request restriction of use and disclosure

- Includes treatment, payment, health care operations
- Covered entity may refuse
- If agrees → bound (except for emergency treatment)

Right to request to receive communications by alternative means or location

- Correspondence sent to alternate address
- Alternative means of communication
- Must permit request and accommodate reasonable requests
  - Health Plan must accommodate if individual endangered
    may require statement to that effect
  - Provider may not require explanation
- Covered entity may require written request

Admin Impacts

Administrative Requirements

- *Implement administrative, technical and physical safeguards*
  - Legal entities with health care components must prevent disclosure to other components not otherwise permitted if they were separate and distinct legal entities
  - must work in tandem with "minimum necessary"
- *Implement policies and procedures to comply with HIPAA*
  - "minimum necessary" coverage for routine disclosures
  - change as necessary to comply with changes in the law
- *Documentation:*
  - all policies and procedures
  - all written communications
  - all required actions
  - all personnel designations
  - maintain for six years

Admin Impacts

Administrative Requirements

Workforce Training and Sanctions

- Training in organization's HIPAA-related PHI policies for:

  - Entire workforce by compliance date
  - New employees following hire
  - Affected employees after material changes in policies

- Privacy and security awareness training to be appropriate for workforce to carry out their functions within the covered entity

- Documentation that training has been provided

Admin Impacts

Administrative Requirements

Additionally, covered entities must:

Complaints --------- Provide a complaint process for individuals

Sanctions ---------- Apply workforce sanctions

Mitigation ---------- Mitigate harmful effects of improper use or disclosure

Retaliation ---------- May not threaten, intimidate, coerce against those exercising rights

Waiver of Rights -- Not require individuals to waive rights

Privacy Official ---- Must designate privacy official and contact person

BA Contracts ------ Must establish permitted uses and disclosures

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Summary

- Change in *status quo*
- Very unlike Y2K:
  - Not only an IT issue — mostly business operations, people & processes
  - No endpoint — progresses from planning to implementation to ongoing compliance
- Balancing act:
  - Compliance obligations with organizational size & capabilities
  - Process improvement opportunities with implementation costs

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

What needs to be done?

1. Make basic decisions
   - Confirm covered status
   - Determine what type of organization you are (e.g., single covered entity, hybrid organization, multi-function, etc.)
2. Begin planning an initial privacy analyses work effort to identify what specific requirements apply your operations.
   - Set within the context of the preemption interplay between HIPAA, State and other Federal laws
3. Utilize the above analysis to assess how new or more stringent requirements will impact operations and what actions are needed to achieve compliance.
4. Decide how to implement the privacy officer function

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

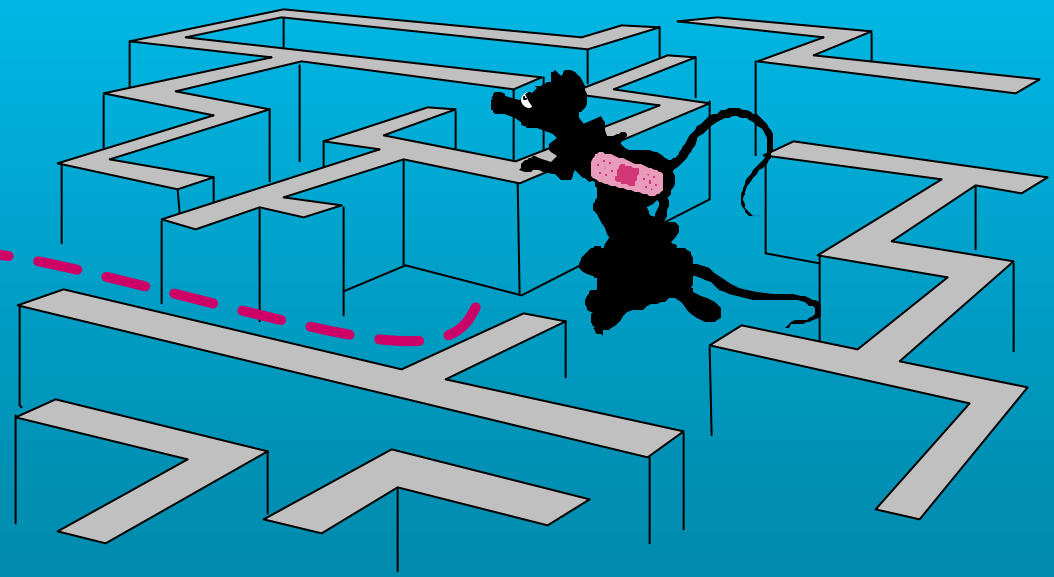
Where do we go from here?

Contracts With Business Associates

Disclosures

Safeguards

Protected Information



Covered Status

Training

Individual Rights

Penalties

Documentation

Preemption

Policies & Procedures

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Basic Decisions

Status Update: DHFS Determinations

The following information is an initial, unconfirmed determination of the HIPAA covered entity status of programs administered by DHFS. These determinations are not final. They may change based upon:

1. Evolving internal legal advisory opinions

2. Opinions from Dept. of Health and Human Services

Basic Decisions

Status Update: DHFS Determinations

Wisconsin DHFS Covered Health Plans:

- Wisconsin Medicaid
- Wisconsin Partnership/PACE
- Wisconsin Family Care
- BadgerCare - Wisconsin State Children's Health Insurance Plan under Title XXI
- Wisconsin Health Insurance Risk Sharing Plan

Basic Decisions

Status Update: DHFS Determinations

What about the Medicaid Home and Community-Based Waiver (HCBW) programs?

HHS states (preamble to the final rule) that they disagree that HCBW services should have a blanket exemption since:

" First, Congress explicitly included the Medicaid programs as health plans.." *

" Second, these waiver programs commonly pay for a mix of health care and non-health care services. State Medicaid agencies with home and community-based waivers are not exempt from these standards for transactions relating to health care services or supplies"

* 65 Fed. Reg. at 50316

Basic Decisions

Status Update: DHFS Determinations

Wisconsin is submitting to HHS its interpretation that:

Our waivers can fund only social and environmental supports and services that Medicaid deems are not medically necessary.

Waiver providers are typically non-traditional and non-health care providers

All health care needs are funded by the Medicaid State Plan

and

The county and tribal agencies that administer the waivers in Wisconsin are not covered entities.

Basic Decisions

Status Update: DHFS Determinations

We are seeking a definitive response from HHS on two fundamental questions:

- Are HIPAA regulations applicable to Wisconsin's home and community-based waiver programs?

- If yes, are the county agencies that administer the waivers considered providers, health plans, business associates, or some other entity?

Basic Decisions

Status Update: DHFS Determinations

We are also asking confirmation of our determination that other programs for which DHFS receives *federal* financial assistance are not considered to be health plans:

Most notable:

- Block Grants for Community Mental Health Services
- Block Grants for Prevention and Treatment of Substance Abuse
- Maternal and Child Health Services Block Grant to States
- Immunization Grants
- Cooperative Agreements for State-based Comprehensive Breast and Cervical Cancer Early Detection

Basic Decisions

Status Update: DHFS Determinations

And confirmation of our determination that the following state programs are not considered to be health plans:

- County General Relief Medical
- Wisconsin Chronic Disease
- Community Options Program, and
- WisconCare

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

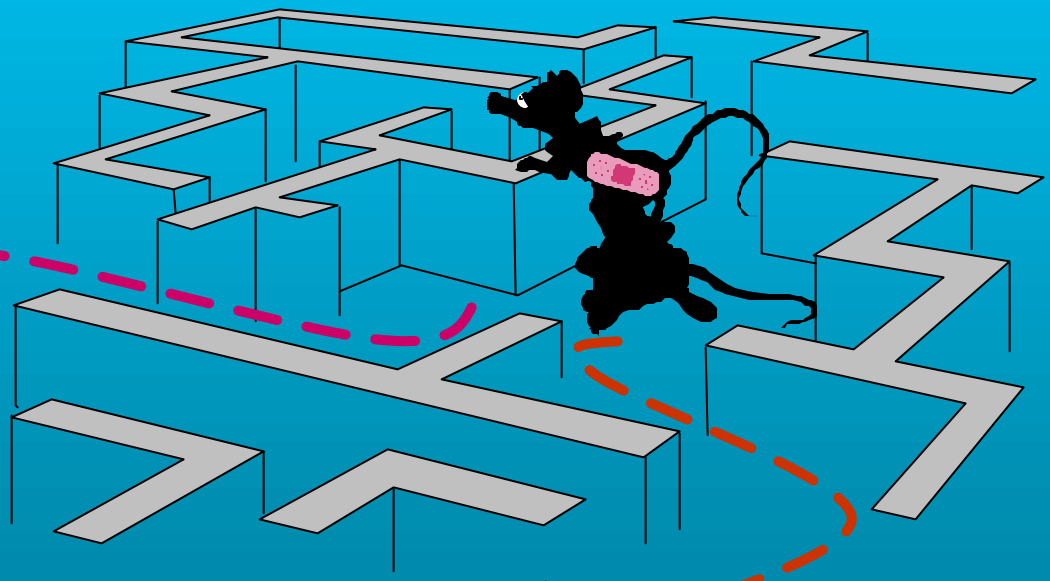
Next?

Contracts With Business Associates

Disclosures

Safeguards

Protected Information



Covered Status

Training

Individual Rights

Penalties

Documentation

Preemption

Policies & Procedures

Next Steps

Preemption Analysis

Since:

- HIPAA adds to the mix of existing federal and state confidentiality laws and preempts any contrary law unless an exception applies

and

- The totality of these laws exercise authority over our operational behavior

We

- Must develop clear requirements of where operations need changing and an understanding of what actions are needed to achieve compliance before proceeding with specific implementations.

Next Steps

DHFS - Preemption Action Plan

- Assemble project team
- Develop an assessment tool and methodology
- Identify:
  - Where exceptions apply
  - Where HIPAA is more stringent
  - Where fed/state laws are more stringent
  - Where HIPAA imposes new requirements
- Determine what needs changing:
  - contracts
  - notice, consent
  - authorizations
  - uses
  - disclosures
  - training
  - policies
  - procedures
  - access, amendment

Next Steps

DHFS - Provider Pilot

Work with the Division of Care and Treatment Facilities to develop/refine assessment tool and methodology.

- Covered Providers
  - Mendota Mental Health Institute
  - Winnebago Mental Health Institute
  - Wisconsin Resource Center
  - Sand Ridge Treatment Center
  - Northern Wisconsin Center
  - Central Wisconsin Center
  - Southern Wisconsin Center

HIPAA: Privacy of Individually Identifiable Health Information
Final Rule: The Basics

Next Steps

Last but not least ...

- Proceed with HIPAA implementations in accordance with our legal advisory opinions.
- Proceed with appointing a privacy officer.
  - An initiative for this fall
    - Define duties and responsibilities
    - Determine organizational placement
- Determine feasibility of a statewide solutions conference.
  - Survey: Should we do this?
    What should be covered or included?
  - If felt need sufficient, would conduct within next six months

Questions?

Contact:

Ted Ohlswager:
phone: (608) 266-5314
e-mail: ohlswts@dhfs.state.wi.us

Rich Ruby:
phone: (608) 267-9044
e-mail: rubyra@dhfs.state.wi.us